FIŞA DISCIPLINEI
AN UNIVERSITAR 2024-2025

1. Date despre program

Instituția de învățământ superior	**Universitatea Maritimă din Constanța**
Școala doctorală	Inginerie Navală și Navigație
Domeniul de studii	Inginerie Navală și Navigație
Ciclul de studii	Doctorat
Programul de studii / calificarea	Inginerie Navală și Navigație/Doctor în Inginerie Navală și Navigație
Forma de învățământ	**IF**

2. Date despre disciplină

Denumirea disciplinei			**Securitatea cibernetică și protecția datelor în ingineria navală și navigație**			
Titularul activităților de curs			Conf.univ.dr. Gabriel Mărgărit Raicu			
Titularul activităților de seminar/laborator/proiect			Conf.univ.dr. Gabriel Mărgărit Raicu			
Anul de studii	1	Semestrul	II	Tipul de evaluare	Examen	
Regimul disciplinei	Categoria de opționalitate a disciplinei: DI - obligatorie (impusă), DO - opțională (la alegere)					DO

3. Timpul total estimat (ore alocate activităților didactice)

I a) Număr de ore pe săptămână	6	Curs	3	Seminar		Laborator	3	Proiect	
I b) Totalul de ore pe semestru din planul de învățământ	84	Curs	42	Seminar		Laborator	42	Proiect	

II Distribuția fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie și notițe	120
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren	90
II c) Pregătire seminare / laboratoare, teme, referate, portofolii și eseuri	81
III Tutorat	
IV Examinări	2
V Alte activități (precizați):	

Total ore studiu individual II (a+b+c)	291
Total ore pe semestru (Ib+II+III+IV+V)	375
Numărul de credite	15

4. Precondiții (acolo unde este cazul)

Curriculum	
Competențe	

5. Condiții (acolo unde este cazul)

Desfășurare a cursului		• PC cu programe specializate • Video-proiector, tablă • Materiale educaționale pentru prezentare, Campusul Virtual al UMC
Desfășurare a aplicațiilor	Seminar	
	Laborator	În sală dotată corespunzător cu tablă, laptop, videoproiector etc. • 30 calculatore cu software specializat; • Simulator Navigație și Manevra Navei • Simulator Cyber Security • Screen display – plasma; • Aplicaţii software cu licență specializate; • Campusul Virtual al UMC – materiale didactice • Prezentări multimedia • Tutoriale video

		• Internet
	Proiect	

6. Competențe specifice acumulate

Competențe profesionale	• Capacitatea de a utiliza concepte, teorii şi modele descriptive şi evaluative pentru explicarea şi interpretarea soluţiilor inginereşti în industria navală și a transportului maritim. • Capacitatea de a analiza procesele fizice ce apar în funcţionarea sistemelor și echipamentelor navale și a transportului maritim. • Capacitatea de a proiecta sistemele din domeniul ingineriei navale, a navigației și a transportului maritim. • Capacitatea de a utiliza şi opera cu instrumente specifice privind tehnicile de optimizare energetică în domeniul ingineriei navale și a navigației. • Capacitatea de aplicare a normelor şi normativelor de siguranţă, securitate şi intervenţie pentru prevenirea poluării produse ca urmare a exploatării navelor maritime şi protejarea mediului marin împotriva deversărilor accidentale și intenționate de la bordul navelor. • Capacitatea de a comunica cu specialiştii din alte domenii, conexe activităţii domeniului inginerie navală şi navigaţie.
Competențe transversale	• Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informației şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii și al adaptării la dinamica cerinţelor acesteia. • Utilizarea eficientă a tehnicilor de relaţionare interumană în cadrul unui colectiv multicultural, pe diverse paliere ierarhice, de comunicare orală şi scrisă, de colaborare eficientă cu specialişti din domenii multiple. • Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare. • Demonstrarea şi aplicarea unei atitudini riguroase, eficiente și responsabile faţă de munca prestată, manifestând un comportament etic, în rezolvarea problemelor şi luarea deciziilor.

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

Obiectivul general al disciplinei	Cunoașterea și înțelegerea problematicii siguranței și securității navelor, a securităţii cibernetice în ingineria navală și navigație, a practicilor specifice la bordul navelor și în companiile din domeniul industriei navale, precum și a procedurilor și mecanismelor de management, a amenințărilor informatice pentru realizarea securității cibernetice
Obiectivele specifice	La finalizarea cu succes a acestei discipline, doctoranzii vor fi capabili să: • Înțeleagă conceptele pe care se bazează managementul riscurilor; • Descrie etapele de pregătire a operațiunilor de răspuns în caz de identificare a potențialelor amenințări; • Identifice și să evalueze critic metodele de răspuns și timpul de reacție în cazul apariției problemelor de securitate cibernetică; • Elaboreze un plan de abordare profesională a problematicii, bazându-se pe metode de cercetare adecvate

8. Conținuturi

Curs	Nr. ore	Metode de predare	Obs
1. Concepte generale privind securitatea informatiei.	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
2. Securitatea informatiei in medii heterogene	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
3. Arhitecturi de retea reziliente Reziliența rețelelor de date	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator

4. Medii de rețea	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
5. Retele wireless si modele de securitate	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
6. Arhitectura retelei Internet	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
7. Sisteme distribuite si concepte generale de securitate	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
8. Securitatea sistemelor izolate	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
9. Criptografie generala	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
10. Vulnerabilități. Identificarea acestora	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
11. Pentesting.	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
12. Raspunsul la incidentele de securitate cibernetica	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
13. Managementul riscului.	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator
14. Politici si standarde	3	Prelegere, dezbatere, explicație; problematizarea; Mijloace de predare: documentații electronice, bază de date cu exemple, metode interactive predare-invatare	Videoproiector, calculator

Bibliografie

- Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.
- "Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian
- Stevens, Tim (2018-06-11). "Global Cybersecurity: New Directions in Theory and Methods". Politics and Governance. 6 (2): 1–4. doi:10.17645/pag.v6i2.1569

- Gabriel Raicu –Unităţi de învăţare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentaţie gratuită accesibilă online, 2022

Bibliografie minimală

Gabriel Raicu –Unităţi de învăţare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentaţie gratuită accesibilă online, 2022

Aplicații (laborator)	Nr. ore	Metode de predare	Obs
Securitatea informatiei, exemple si aplicatii	6	Studiu de caz, dezbatere, problematizare, Utilizarea Campusului Virtual UMC Lucrul individual şi în echipe	Videoproiector, calculator
Schimbul de date in medii eterogene	6	Studiu de caz, dezbatere, problematizare, Utilizarea Campusului Virtual UMC Lucrul individual şi în echipe	Videoproiector, calculator
Arhitecturi de retea si elemente de propagare a riscurilor	6	Studiu de caz, dezbatere, problematizare, Utilizarea Campusului Virtual UMC Lucrul individual şi în echipe	Videoproiector, calculator
Sisteme criptografice, algortimi si viteza de calcul	6	Studiu de caz, dezbatere, problematizare, Utilizarea Campusului Virtual UMC Lucrul individual şi în echipe	Videoproiector, calculator
Securitatea informatiei, tehnici de obfuscare si steganografie	6	Studiu de caz, dezbatere, problematizare, Utilizarea Campusului Virtual UMC Lucrul individual şi în echipe	Videoproiector, calculator
Pentesting. Exemple si aplicatii live	6	Studiu de caz, dezbatere, problematizare, Utilizarea Campusului Virtual UMC Lucrul individual şi în echipe	Videoproiector, calculator
Adresarea riscurilor si paradigme legislative asociate	6	Studiu de caz, dezbatere, problematizare, Utilizarea Campusului Virtual UMC Lucrul individual şi în echipe	Videoproiector, calculator

Bibliografie

- Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.
- "Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian
- Stevens, Tim (2018-06-11). "Global Cybersecurity: New Directions in Theory and Methods". Politics and Governance. 6 (2): 1–4. doi:10.17645/pag.v6i2.1569
- Gabriel Raicu –Unităţi de învăţare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentaţie gratuită accesibilă online, 2022

Bibliografie minimală

Gabriel Raicu –Unităţi de învăţare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentaţie gratuită accesibilă online, 2022

15. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

În vederea schițării conținuturilor, alegerii metodelor de predare/învățare titularii disciplinei au consultat conținutul unor discipline similare predate la universitati din străinătate. Cursul indeplineste cerintele minime de cunoastere si intelegere recomandate de către EMSA (European Maritime Safety Agency), IMO (Internationbal Maritime Organisation), BIMCO (Baltic and International Maritime Council Organisation), ENISA (The European Union Agency for Cybersecurity), precum și a altor organizații cu preocupări în domeniu.

16. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- Claritatea, coerenta si concizia expunerii; - Utilizarea corecta a conceptelor fundamentale; - Abilitatea de a opera cu notiuni de baza.	Elaborarea și prezentarea unui referat	80%
Laborator	Planificarea corectă a operațiunilor de identificare și răspuns în caz de atac cibernetic la bordul navei	Verificarea, observație pe durata activității de laborator	20%
Standard minim de performanță			
Generarea și analiza unui set de date simulate autentice în cadrul unui atac atac cibernetic identificat la bordul navei – minim calificativ Bine			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar/laborator/proiect
24.06.2024	Conf.univ.dr. Gabriel Raicu	Conf.univ.dr. Gabriel Raicu

Data aprobării în CSUD	Semnătura DSUD
27.06.2024	Conf.univ.dr. Nicoleta Acomi